IOS VPN (router): Voeg een nieuwe L2L-tunneltoegang of externe toegang toe aan een bestaande L2L VPN

Inhoud

Inleiding

Dit document biedt de stappen die vereist zijn om een nieuwe L2L VPN-tunnel of een externe VPN-toegang toe te voegen aan een L2L VPN-configuratie die al in een IOS-router bestaat.

Voorwaarden

Vereisten

Zorg ervoor dat u correct de L2L IPSec VPN-tunnel vormt die momenteel operationeel is voordat u deze configuratie probeert.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Twee IOS-routers die softwareversies 12.4 en 12.2 uitvoeren

- Eén Cisco adaptieve security applicatie (ASA) met softwareversie 8.0

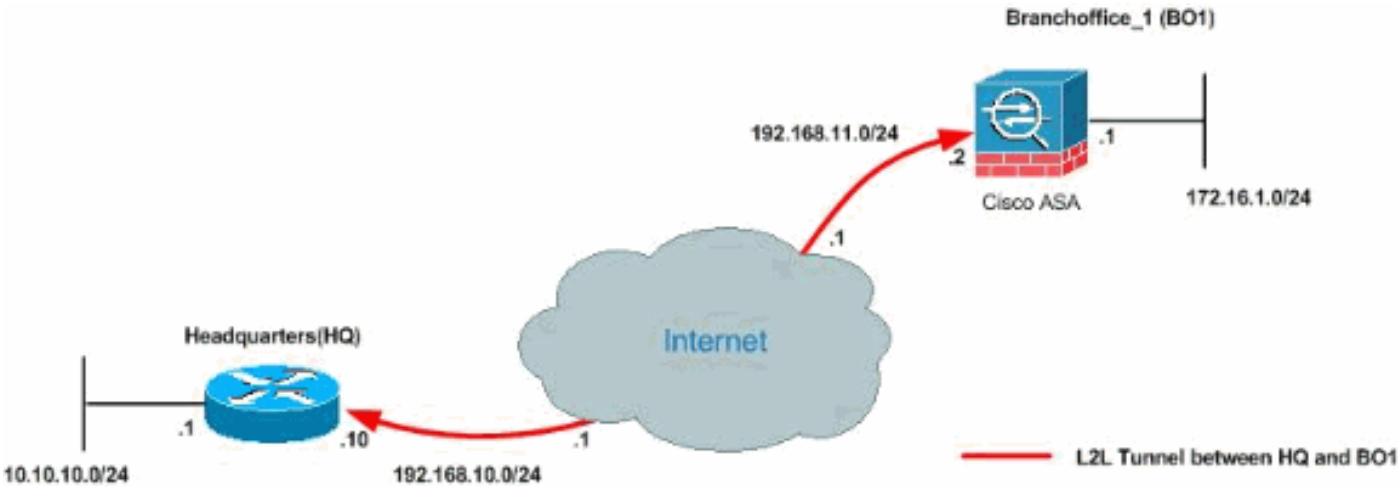
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Deze output zijn de huidige actieve configuraties van de router van het Hoofdkantoor (HUB) en de ASA van het Vestigingskantoor 1 (BO1). In deze configuratie is er een IPSec L2L-tunnel ingesteld tussen HQ en BO1 ASA.

Configuratie van huidige HQ (HUB)-router

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
```

```
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
!
!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

ASA-configuratie

```
CiscoASA#show running-config
```

```
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
```

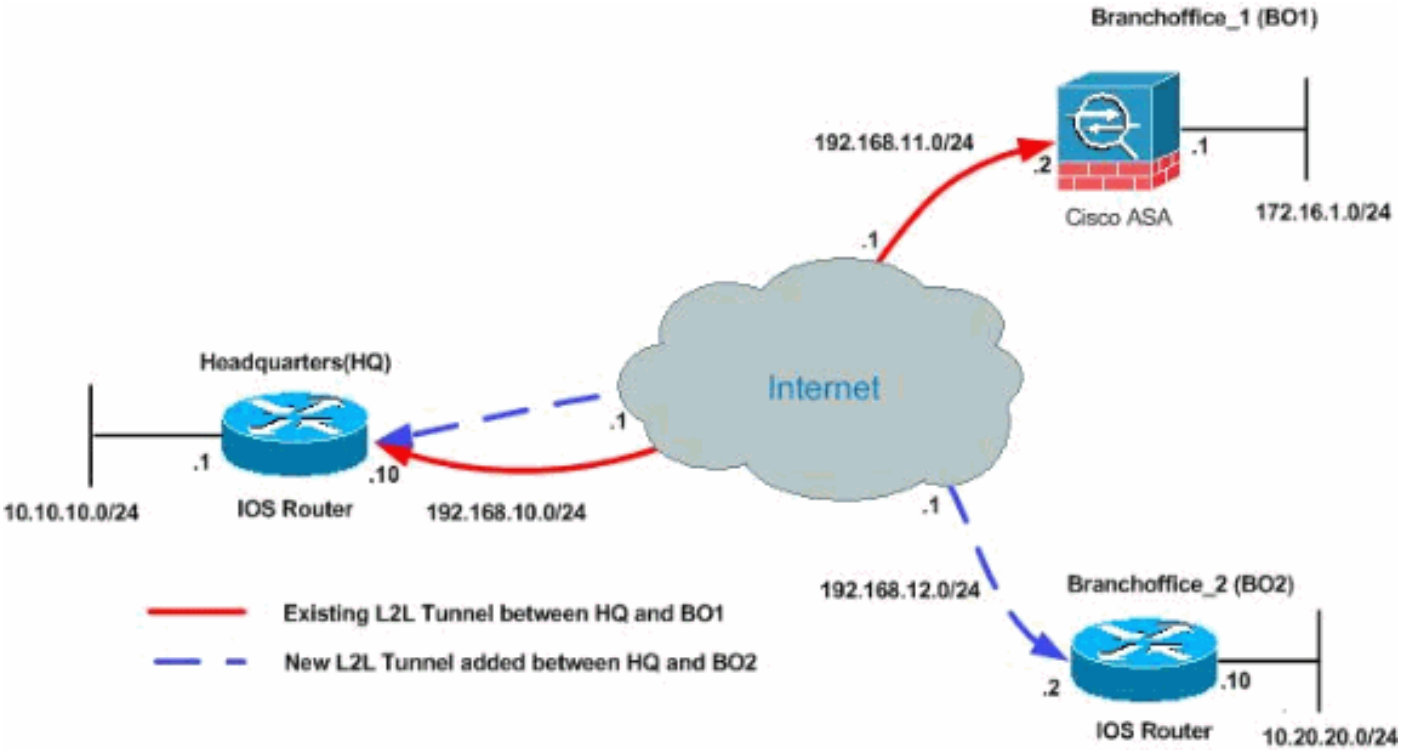
```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

Achtergrondinformatie

Momenteel is er een bestaande L2L-tunnel opgezet tussen het kantoor van het hoofdkwartier en het kantoor van het hoofdkwartier. Uw bedrijf heeft onlangs een nieuw bijkantoor geopend (BO2). Dit nieuwe kantoor vereist connectiviteit met lokale middelen die in het kantoor van het Hoofdkantoor zijn gevestigd. Daarnaast is er een aanvullende verplichting om werknemers de mogelijkheid te geven om van huis te werken en veilig toegang te krijgen tot middelen die zich op afstand op het interne netwerk bevinden. In dit voorbeeld wordt een nieuwe VPN-tunnel zo ingesteld dat er ook een VPN-server voor externe toegang wordt geïnstalleerd die zich in het kantoor van het hoofdkwartier bevindt.

Voeg een extra L2L-tunnel toe aan de configuratie

Dit is het netwerkdiagram voor deze configuratie:



Stapsgewijze instructies

Deze sectie verschaft de gewenste procedures die moeten worden uitgevoerd op de HUB Q router.

Voer de volgende stappen uit:

1. Maak deze nieuwe toegangslijst die door de crypto map gebruikt moet worden om interessant verkeer te definiëren:
   ```
   HQ_HUB(config)#ip access-list extended VPN_BO2
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   ```

   Waarschuwing: om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang (toegangscontrolelijst) voor dat specifieke netwerk hebben.
2. Voeg deze ingangen aan het nee nat statement toe om het ding tussen deze netwerken vrij te stellen:
   ```
   HQ_HUB(config)#ip access-list extended NAT_Exempt
   HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
   ```

   Voeg deze ACLs aan de bestaande routekaart **nonat toe**:
   ```
   HQ_HUB(config)#route-map nonat permit 10
   HQ_HUB(config-route-map)#match ip address NAT_Exempt
   HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
   ```

   Waarschuwing: om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang voor dat specifieke netwerk hebben.
3. Specificeer het peer adres in de fase 1 configuratie zoals weergegeven:
   ```
   HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
   ```

Opmerking: de pre-gedeeld toets moet precies aan beide zijden van de tunnel overeenkomen.

4. Maak de crypto kaartconfiguratie voor de nieuwe VPN-tunnel. Gebruik dezelfde transformatie die gebruikt werd in de eerste VPN-configuratie, aangezien alle fase 2-instellingen hetzelfde zijn.

```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
 HQ_HUB(config-crypto-map)#set peer 192.168.12.2
 HQ_HUB(config-crypto-map)#set transform-set newset
 HQ_HUB(config-crypto-map)#match address VPN_BO2
```

5. Nu je de nieuwe tunnel hebt ingericht, moet je interessant verkeer door de tunnel sturen om hem omhoog te halen. Om dit uit te voeren, geef de uitgebreide **ping** opdracht uit om een host op het binnennetwerk van de afstandstunnel te pingelen.In dit voorbeeld is een werkstation aan de andere kant van de tunnel met het adres 10.20.20.16 gepingd. Dit brengt de tunnel op tussen HQ en BO2. Nu zijn er twee tunnels verbonden met het kantoor van het hoofdkwartier. Als u geen toegang hebt tot een systeem achter de tunnel, raadpleeg de meest gebruikelijke L2L- en afstandsbediening van IPSec VPN-probleemoplossing om een alternatieve oplossing te vinden door `beheertoegang`.

Configuratievoorbeeld

HUB_HQ - Voeg een nieuwe L2L VPN-tunnelconfiguratie toe

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
```

```
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

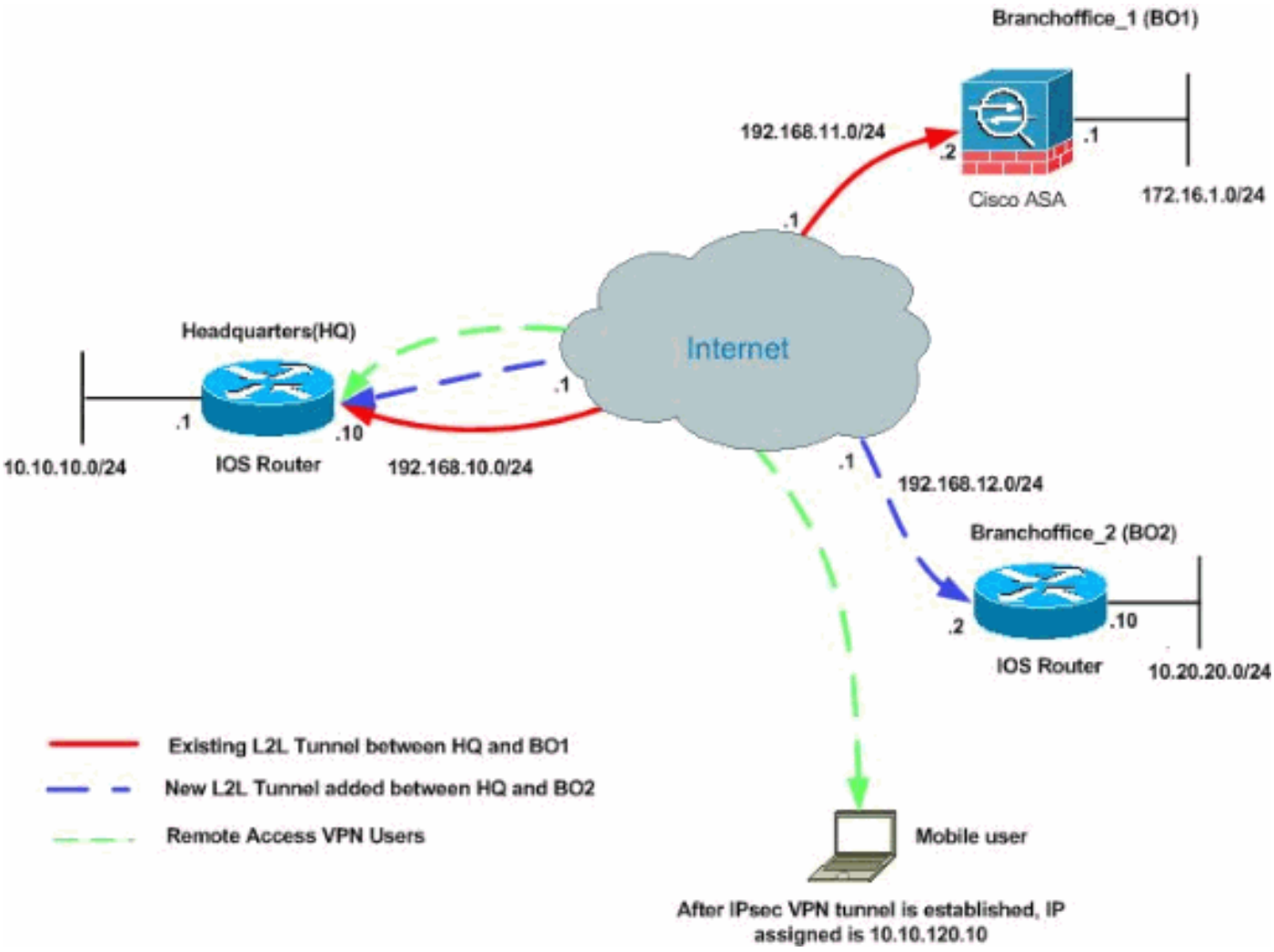
Configuratie van BO2 L2L VPN-tunnelbeheer

```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip nat inside source route-map nonat interface Ethernet1
overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
```

```
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

Een VPN-toegang op afstand toevoegen aan de configuratie

Dit is het netwerkdiagram voor deze configuratie:



In dit voorbeeld wordt de functie **split-tunneling** gebruikt. Deze optie geeft een IPSec-client op afstand toegang tot pakketten voorwaardelijk via een IPSec-tunnel in gecodeerde vorm, of naar

een netwerkinterface in duidelijke tekstvorm. Als gesplitste tunneling ingeschakeld is, hoeven pakketten die niet gebonden zijn voor bestemmingen aan de andere kant van de IPSec-tunnel niet te worden versleuteld, over de tunnel te worden verzonden, te worden gedecrypteerd en vervolgens naar een eindbestemming te worden verzonden. Dit concept past het splitsingstunnelbeleid toe op een bepaald netwerk. De standaardinstelling is om al het verkeer te tunnelen. Om een gesplitst tunneling-beleid in te stellen, specificeert u een ACL waarbij het voor internet bedoelde verkeer kan worden vermeld.

Stapsgewijze instructies

Dit deel bevat de vereiste procedures om de mogelijkheden voor toegang op afstand toe te voegen en om externe gebruikers toegang te geven tot alle sites.

Voer de volgende stappen uit:

1. Maak een IP-adrespool die gebruikt moet worden voor clients die via de VPN-tunnel verbonden zijn. Maak ook een basisgebruiker om toegang tot VPN te krijgen zodra de configuratie is voltooid.
```
HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50


HQ_HUB(config)#username vpnuser password 0 vpnuser123
```
2. Uitzondering van het specifieke verkeer op het feit dat het wordt geregistreerd.
```
HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit
```
   Voeg deze ACLs aan de bestaande routekaart **nonat toe**:
```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```
   Merk op dat de communicatie tussen VPN-tunnels in dit voorbeeld is vrijgesteld.
3. Laat communicatie tussen de bestaande L2L-tunnels en VPN-gebruikers met externe toegang toe.
```
HQ_HUB(config)#ip access-list extended VPN_BO1
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```
   Dit staat verre toegangsgebruikers de mogelijkheid toe om met netwerken achter de gespecificeerde tunnels te communiceren.**Waarschuwing:** om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang voor dat specifieke netwerk hebben.
4. **Gesplitste tunneling configureren**Om het splitsen tunnelen voor de VPN-verbindingen mogelijk te maken, moet u een ACL op de router configureren. In dit voorbeeld wordt de **toegang-lijst split_tunnel** opdracht geassocieerd met de groep voor split-tunneling

doeleinden, en de tunnel gevormd tot de 10.10.10.0/24 en 10.20.20.0/24 en 172.16.1.0/24 netwerken. Verkeersstromen niet versleuteld met apparaten die niet in een gesplitste ACL-tunnel (bijvoorbeeld het internet).

```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

5. Configuratie van lokale authenticatie, vergunning en clientconfiguratie informatie, zoals wins, dns. Interessant verkeersknooppunt en IP-pool voor de VPN-clients.

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```

6. Configureer de dynamische kaart en de cryom informatie die vereist is voor de maken van de VPN-tunnel in kaart te brengen.

```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

Configuratievoorbeeld

Voorbeeld Configuration 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
```

```
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
```

```
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255



!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **ping**-Deze opdracht staat u toe om de L2L VPN-tunnel te openen zoals wordt getoond.

Problemen oplossen

Raadpleeg deze documenten voor informatie die u kunt gebruiken om problemen met uw configuratie op te lossen:

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- IP-beveiligingsprobleemoplossing - Oplossingen begrijpen en gebruiken van debug-opdrachten

Tip: Als u beveiligingsassociaties reinigt en u geen IPsec VPN-kwestie oplost, verwijdert en opnieuw toepast u de betreffende crypto-map om een brede reeks problemen op te lossen.

Waarschuwing: Als u een crypto kaart van een interface verwijdert, brengt het alle IPSec tunnels neer die geassocieerd zijn met die crypto kaart. Volg deze stappen met voorzichtigheid en overweeg het veranderingscontrolebeleid van uw organisatie voordat u verdergaat.

Voorbeeld

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Gerelateerde informatie

- Een Inleiding aan IP Security (IPSec) encryptie
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Een IPsec router Dynamic LAN-to-LAN peer en VPN-clients configureren
- Technische ondersteuning en documentatie – Cisco Systems